Goals of Compsec

Confidentiality

Integrity

Availability

Types of Compsec Attacks

Interception:unauthorized party gets asset(theft, copying, surveillance)

Interruption:asset unusable(DDos, deletion)

Modification:asset changed(edit files,trapdoor,logic,virus)

Fabrication:fake asset planted(computer,software,records)

Basic Types of Crypto

Symmetric key:des,aes,blowfish,rc5,rc6

Asymmetric:rsa,el-gamal.elliptic curve(slower than sym)

Secure hash:md5,sha1,sha256,ripemd

Collision

Weak:difficult to find text with same hash as a random text

Strong:difficult to find pairs of text with same hash

Crypto Analysis

etaoinshrdlu

bigrams,trigrams(the,and),

index of coincidence(3.8% vs 6.6%)

Types of Attacks on Crypto

ciphertext only, known plaintext, chosen plaintext, chosen ciphertext, dumpster diving, social engineering, threats/blackmail/torture/bribes

Entropy

Entropy:info in message,(Ex, 3.6 bits for a month)

Rate: R = log2 Z, where Z is the size of the alphabet

Abs Rate:how much info, r=H(M)/N where M is an N-bit message.

Redundancy: D = R – r!

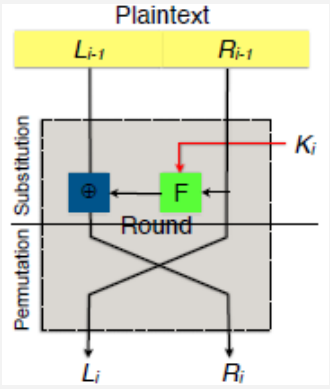
Unicity: amount of cipher needed to find plaintext U = H(K) / D!

Block Ciphers

Diffusion, small changes cause large effects

Confusion, statistics between key and cipher hidden

Feistel



DES

Adopted by NIST 1976 (IBM Lucifer), NSA reduced key from 128 to 56

Feistel with additional initial permutation, 16 rounds, complex f, 48b subkeys

32b >Expand and permute> 48b (Kn) > Substitute (using S boxes) > 32 bits > Permutation

Bruteforce in <24 hours in '96, double DES still too small (2^57)

3DES, slow, almost secure? nsa backdoors?

AES

NIST '96, replace DES, secure 50-100y, faster des, variable key size, block ciph

MARS,RC6,Rijndael,serpent,twofish(key dependent sbox)

blowfish:64b block, fast, still secure, used ssh and openbsd

rijndael doesnt use constant but theyre good pseudorandom, infinite, public no trapdoors

Round: swap state using sbox, cyclic shift each state row, invertible trans each row, XOR state by round key

Modes

ECB: all blocks encrypted independently, identical blocks encrypted identically!

CBC: each block is used next block, more secure

OBC: feedback independent of plaintext, can parallelize

CTR:nonce+counter instead of feedback, very parallel, stream is safe

XEX:efficient,fast,parallel, Cs,j = EK (PS,j ⊕ X) ⊕ X where X = EK (S) ⊗ αj

Side Channel Cryptanalysis

Detect power use, time delay, radiation

Diffie-Hellman

agree on q = large prime, a = random generator

A gets random X sends a^X mod q to B

B gets random Y sends a^Y mod q to A

Each one calculates $(a^X)^Y$ mod q = K

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com

RSA

E(M) = M mod n, D(C) = C mod n

n = p × q p, q are prime

d is relatively prime to (p - 1)(q - 1)

e × d ≡ 1 mod ((p - 1)(q - 1))

hard to factor, getting easier, quantum comp is risk

test

test

testtt

test

By **[deleted]**
cheatography.com/deleted-19894/

Not published yet.
Last updated 7th November, 2014.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com